



Federal CIO Council  
Information Security and Identity Management Committee

# Identity, Credential, and Access Management

## Open Identity Solutions Trust Frameworks

March 9, 2011

Chris Loudon



## Agenda

- Policy Foundation
- Portable Identity Approach
  - Technology
  - Trust
- Implementation



## Policy Foundation: OMB M04-04 E-Authentication Guidance for Federal Agencies

- Defines 4 Assurance Levels
- *“Agencies should determine assurance levels using the following steps, (described in Section 2.3):*
  1. *Conduct a risk assessment of the e-government system.*
  2. *Map identified risks to the applicable assurance level.*
  3. *Select technology based on e-authentication technical guidance.*
  4. *Validate that the implemented system has achieved the required assurance level.*
  5. *Periodically reassess the system to determine technology refresh requirements. “*



# Identity, Credential, and Access Management

## Policy Foundation: OMB M04-04

### FIPS 199 Risk/Impact Profiles

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High



# Identity, Credential, and Access Management

## Policy Foundation: NIST Special Pub 800-63

### ➤ SP 800-63 Technical Guidance

#### *Assurance Level*

<i>Allowed Token Types</i>	1	2	3	4
Hard crypto token	√	√	√	√
One-time Password Device	√	√	√	
Soft crypto token	√	√	√	
Password & PINs	√	√		



# Identity, Credential, and Access Management

## Agenda

- ✓ Policy Foundation
- Portable Identity Approach
  - Technology
  - Trust
- Implementation



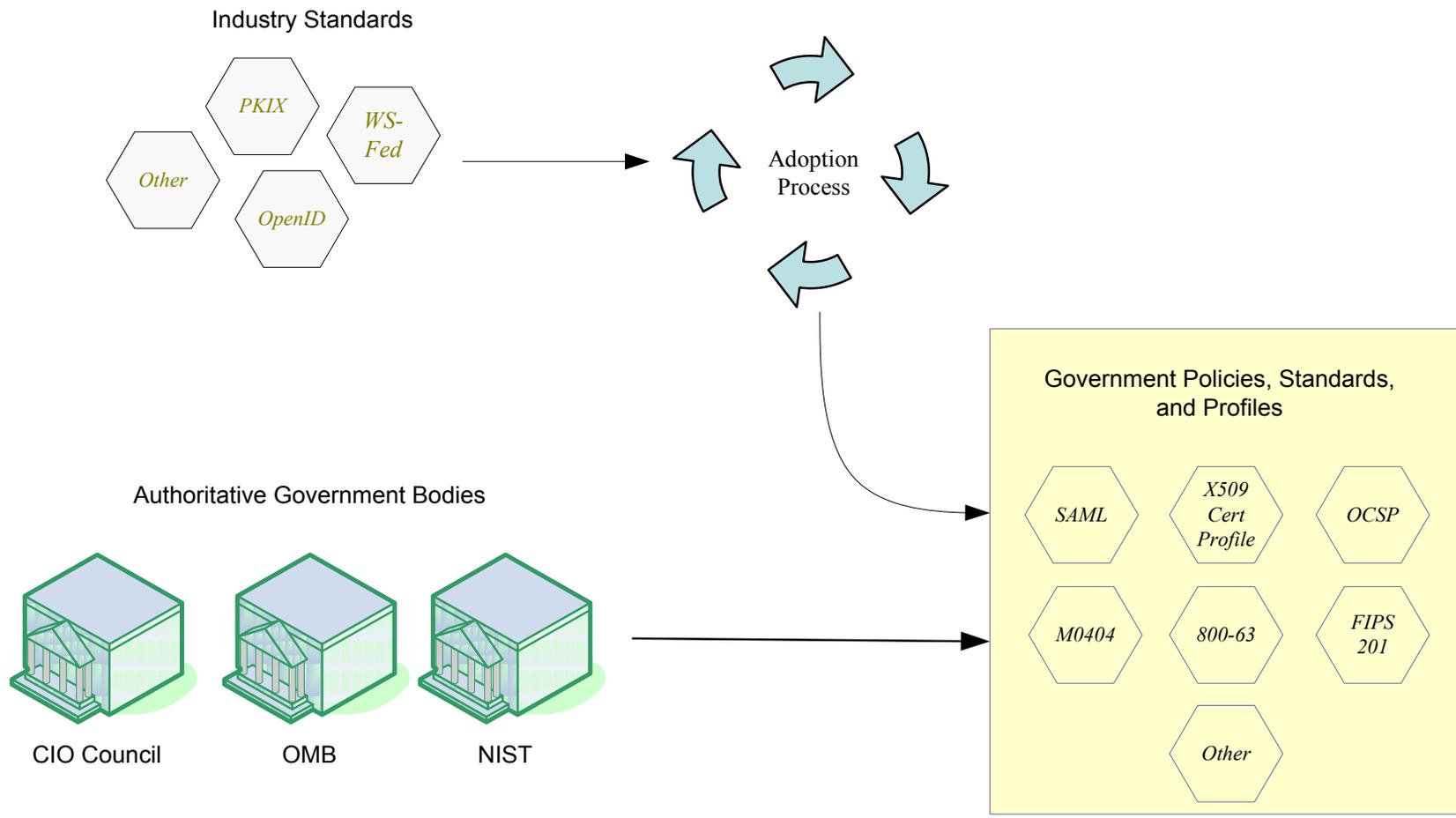
## Approach

- Adopt technologies in use by industry
  - “Scheme Adoption”
- Adopt industry Trust Models
  - “Trust Framework Adoption”
  
- ❖ Approach documents posted on <http://www.IDmanagement.gov>



# Identity, Credential, and Access Management

## Approach: Scheme Adoption





## Approach: Scheme Adoption

### ➤ Scheme Adoption

- Scheme – specific type of authentication token and associated protocols (e.g. user ID & password; PKI; SAML assertion)
- Scheme Adoption produces a *Federal Profile*
- Profile defines MUSTs, SHOULDs, SHOULD NOTs, etc. for Identity Providers (IdPs) & Relying Parties (RPs)
  - *Goal is not to change the existing technical standard*
- Profiles complete for OpenID, Information Card (IMI), and SAML.

❖ *Federal ICAM Identity Scheme Adoption Process* and scheme profiles posted on <http://www.IDmanagement.gov>



# Identity, Credential, and Access Management

## Agenda

- ✓ Policy Foundation
- Portable Identity Approach
  - ✓ Technology
  - Trust
- Implementation



## Approach: Trust Framework Adoption

- Trust Framework Adoption
  - Adoption of Industry Trust Frameworks
  - Adopts at Assurance Levels
  - Considers requirements of NIST SP 800-63
  - Trust Framework Evaluation Team (TFET) reviews applications
- Privacy Principles included
  - Opt in
  - Minimalism
  - Activity Tracking
  - Adequate Notice
  - Non Compulsory
  - Termination
- ❖ *Federal ICAM Trust Framework Provider Adoption Process posted on <http://www.IDmanagement.gov>*



## Approach: Trust Framework Adoption

- Adopted Trust Framework Providers
  - Open Identity Exchange (OIX)  
(<http://openidentityexchange.org/>)
  - Kantarra Initiative (<http://kantarainitiative.org/>)
  - InCommon in progress (<http://www.incommonfederation.org/>)
  
- ❖ Approved Trust Framework Providers and Identity Providers  
posted on <http://www.IDmanagement.gov>



# Identity, Credential, and Access Management

## Kantara

### Trustees



Leadership Council Representatives: Colin Wallis, John Bradley

### Member Organizations





# Identity, Credential, and Access Management

## Open Identity Exchange

### Executive Members

The AT&T logo, consisting of a blue and white globe icon followed by the text "at&t" in a lowercase, sans-serif font.	Booz   Allen   Hamilton
The CA Technologies logo, featuring a stylized "ca" in blue and green, with the word "technologies" in a smaller green font below it.	<b>EQUIFAX</b>
The Google logo, with its characteristic multi-colored letters: G (blue), o (red), o (yellow), g (blue), l (green), e (red).	<b>PayPal™</b>
The Symantec logo, featuring a yellow and black circular icon followed by the text "symantec." in a lowercase, sans-serif font.	<b>verizon</b>
The TNS logo, featuring a black square with white lines radiating from the top right corner, and the letters "TNS" in white below it. Below the logo is the text "Transaction Network Services".	The LexisNexis logo, featuring a red sphere icon followed by the text "LexisNexis" in a sans-serif font.



# Identity, Credential, and Access Management

## InCommon

- 202 Education Participants, 8 Govt/Non-Profit, 72 Sponsored Partners
- 5 million users

### Current InCommon Participants

A community of more than 5 million end users.

*(Source: Higher Education Students, Faculty, and Staff, Integrated Postsecondary Education Data System. Calculated October 2010.)*

Higher Education Participants (202)	Government and Nonprofit Laboratories, Research Centers, and Agencies (8)	Sponsored Partners (72)
<ul style="list-style-type: none"> <li><a href="#">American University</a></li> <li><a href="#">Arizona State University</a></li> <li><a href="#">Augsburg College</a></li> <li><a href="#">Baylor College of Medicine</a></li> <li><a href="#">Baylor University</a></li> <li><a href="#">Boise State University</a></li> <li><a href="#">Brown University</a></li> <li><a href="#">California Institute of Technology</a></li> <li><a href="#">California Maritime Academy</a></li> <li><a href="#">California Polytechnic State University, San Luis Obispo</a></li> <li><a href="#">California State Polytechnic University, Pomona</a></li> <li><a href="#">California State University, Bakersfield</a></li> <li><a href="#">California State University, Channel Islands</a></li> <li><a href="#">California State University, Chico</a></li> <li><a href="#">California State University, Dominguez Hills</a></li> <li><a href="#">California State University, East Bay</a></li> <li><a href="#">California State University, Fresno</a></li> <li><a href="#">California State University, Fullerton</a></li> <li><a href="#">California State University, Long Beach</a></li> <li><a href="#">California State University, Los Angeles</a></li> <li><a href="#">California State University, Monterey Bay</a></li> <li><a href="#">California State University, Northridge</a></li> <li><a href="#">California State University, Office of the Chancellor</a></li> <li><a href="#">California State University, Sacramento</a></li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Argonne National Laboratory</a></li> <li><a href="#">Energy Sciences Network (ESNet)</a></li> <li><a href="#">Fermi National Accelerator Laboratory</a></li> <li><a href="#">Lawrence Berkeley National Laboratory</a></li> <li><a href="#">Moss Landing Marine Laboratories</a></li> <li><a href="#">National Institutes of Health</a></li> <li><a href="#">National Science Foundation</a></li> <li><a href="#">TeraGrid</a></li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Absolute Software, Inc.</a></li> <li><a href="#">ALEKS Corporation</a></li> <li><a href="#">Alexander Street Press</a></li> <li><a href="#">Apple - iTunes U</a></li> <li><a href="#">Atlas Systems, Inc.</a></li> <li><a href="#">BioOne, Inc.</a></li> <li><a href="#">Blackboard, Inc.</a></li> <li><a href="#">Blatant Media Corporation</a></li> <li><a href="#">Burton Group</a></li> <li><a href="#">Cambridge University Press</a></li> <li><a href="#">Cayuse, Inc.</a></li> <li><a href="#">Cengage Learning, Inc.</a></li> <li><a href="#">Colorado Alliance of Research Libraries</a></li> <li><a href="#">CSO Research, Inc.</a></li> <li><a href="#">Davie County Schools</a></li> <li><a href="#">Desire2Learn</a></li> <li><a href="#">Digital Measures</a></li> <li><a href="#">Docufide, Inc.</a></li> <li><a href="#">e-academy, Inc.</a></li> <li><a href="#">e2Campus by Omnilert, LLC</a></li> <li><a href="#">Ebook Library - EBL</a></li> <li><a href="#">EBSCO Publishing</a></li> <li><a href="#">EDUCAUSE</a></li> <li><a href="#">Elsevier</a></li> </ul>



# Identity, Credential, and Access Management

## Approach: Trust Framework Adoption

### ➤ Approved Identity Providers

IDP	LOA	Scheme	TFP
Google	1	OpenID	OIX
Equifax	1	IMI, OpenID	OIX
Paypal	1	IMI, OpenID	OIX
Verisign	1	OpenID	OIX
Wave	1	OpenID	OIX

❖ Approved Trust Framework Providers and Identity Providers posted on <http://www.IDmanagement.gov>



# Identity, Credential, and Access Management

## Agenda

- ✓ Policy Foundation
- ✓ Portable Identity Approach
  - ✓ Technology
  - ✓ Trust
- Implementation



## Implementation

- Determine LOA for your application
  - M -04-04 levels of assurance
- Review Privacy Impact Assessment
  - use of third party credentials may effect PIA



## Implementation

- Implement the appropriate scheme
  - e.g. “OpenID Enable” your site
  - OpenID, SAML, IMI Profiles on [idmanagement.gov](http://idmanagement.gov)
  - Open Source, Free Libraries, Platform Modules, Commercial Products available
  - Schemes should be integrated into your existing application, probably by your existing web team
  - Details depend on how you built your website
  - Consider which IDPs support which schemes
  - Help available from the ICAM SC Lab



## Implementation Considerations

- Configure metadata for approved IDPs
  - URLs, Configuration information for each IDP
  - Coordinate through ICAM SC Lab
- Consider User Interface (UI)



# Identity, Credential, and Access Management

## Implementation Considerations



My NCBI - Home - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.ncbi.nlm.nih.gov/sites/myncbi/

Most Visited Getting Started Latest Headlines

IDManagement.gov Yahoo! Mail: The best web-based email! My NCBI - Home

NCBI Home PubMed GenBank BLAST Sign In | My NCBI

**My NCBI** A division of the National Library of Medicine at the National Institutes of Health

Table of Contents Welcome to My NCBI

**My NCBI Home**

My Saved Data

Search Filters

Preferences

About My NCBI

Use My NCBI to save your searches and data, and to set NCBI Web site preferences [About My NCBI...](#)

Sign in directly to your My NCBI account:

**My NCBI Sign In**

Username:

Password:

Keep me signed in unless I sign out (Leave unchecked on public computers)

Remember my username

[Register for an account](#)

[I forgot my username](#)

[I forgot my password](#)

[About automatic sign in](#)

or

Register or sign in through one of the partner organization login routes:

**Sign in via Partner Organization**

[Google](#)

[NIH Login](#)

[eRA Login](#)

[UKPMC Funders Group grantees](#)

**Or choose from:**

Case Western Reserve University

Colorado State University

Columbia University

Cornell University

[See expanded list](#)



# Identity, Credential, and Access Management

## Implementation Considerations



The screenshot displays a web browser window with the following elements:

- Browser Title:** Yahoo! Mail: The best web-based email! - Mozilla Firefox
- Address Bar:** https://login.yahoo.com/config/login\_verify2?&.src=ym
- Page Content:**
  - Yahoo! logo and navigation links (Yahoo! | Help)
  - Advertisement: "Go anywhere. Your emails will follow. Yahoo! Mail Beta is here. Now available to try from your Yahoo! Mail"
  - Form titled "Don't have a Yahoo! ID?" with a "Create New Account" button.
  - Form titled "Sign in to Yahoo!" with fields for "Yahoo! ID" (with example: free2rhyme@yahoo.com) and "Password".
  - Checkbox: "Keep me signed in (Uncheck if on a shared computer)"



## Implementation Considerations

### ➤ Not rocket science

- thousands of sites have implemented these technologies
- does require attention from your web team
- will impact release planning
- does not require new commercial software, servers, bandwidth, capital expenditures, etc
- impact similar to any new feature integrated into your site



## Agenda

- ✓ Policy Foundation
- ✓ Portable Identity Approach
  - ✓ Technology
  - ✓ Trust
- ✓ Implementation
- Questions?



# Identity, Credential, and Access Management

## Backup Slides



## Backup Slides

➤ [Scheme Details](#)



## Portable Identity Schemes: SAML

### ➤ SAML

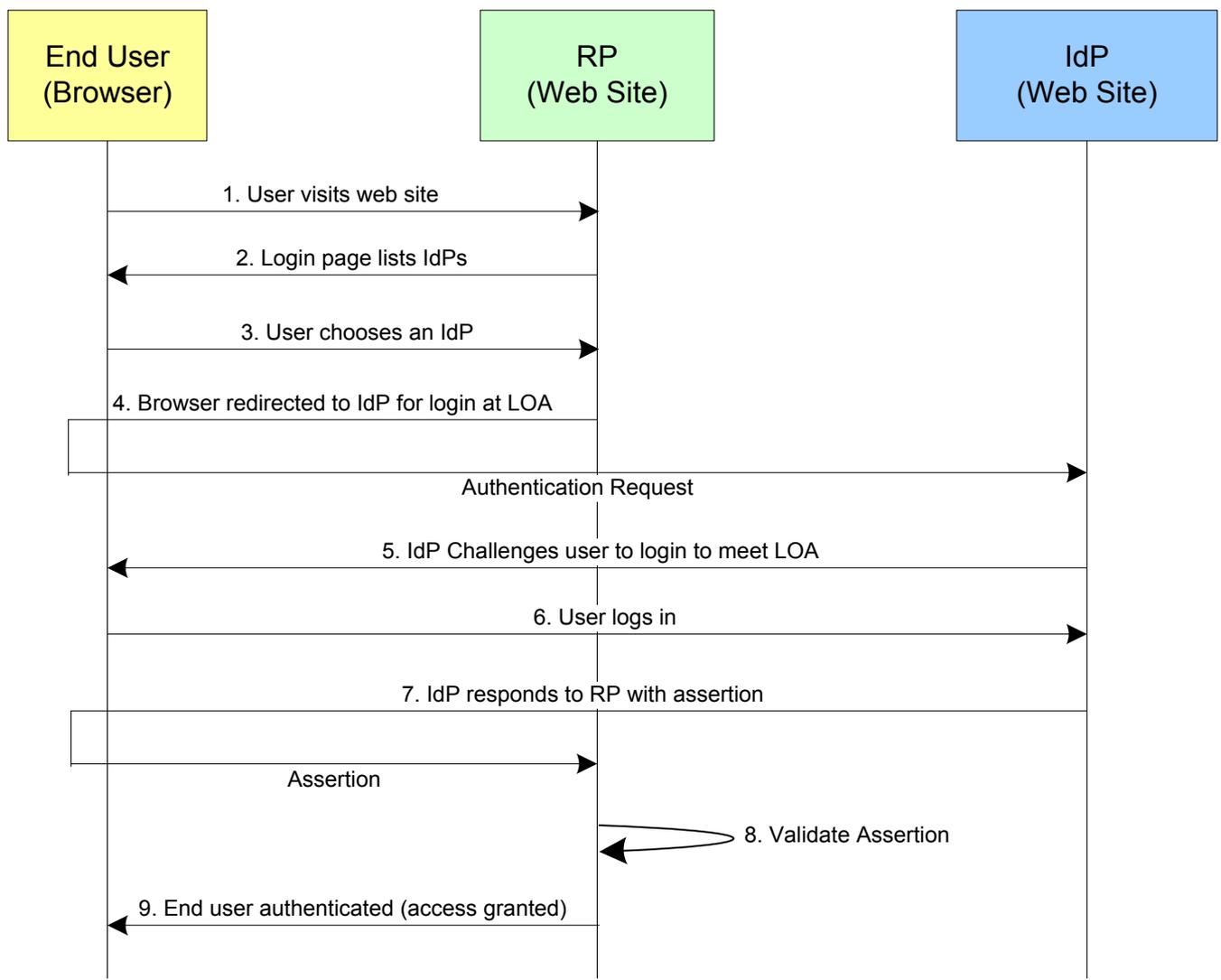
- OASIS SAML 2.0
- Based on E-Gov Profile developed through Liberty
- Broad COTS support
- Has been used by government before

### ➤ Federal Profile

- Requires E-Gov Profile
- Requires encryption of PII



# Portable Identity Schemes: SAML





## Portable Identity Schemes: OpenID

### ➤ OpenID

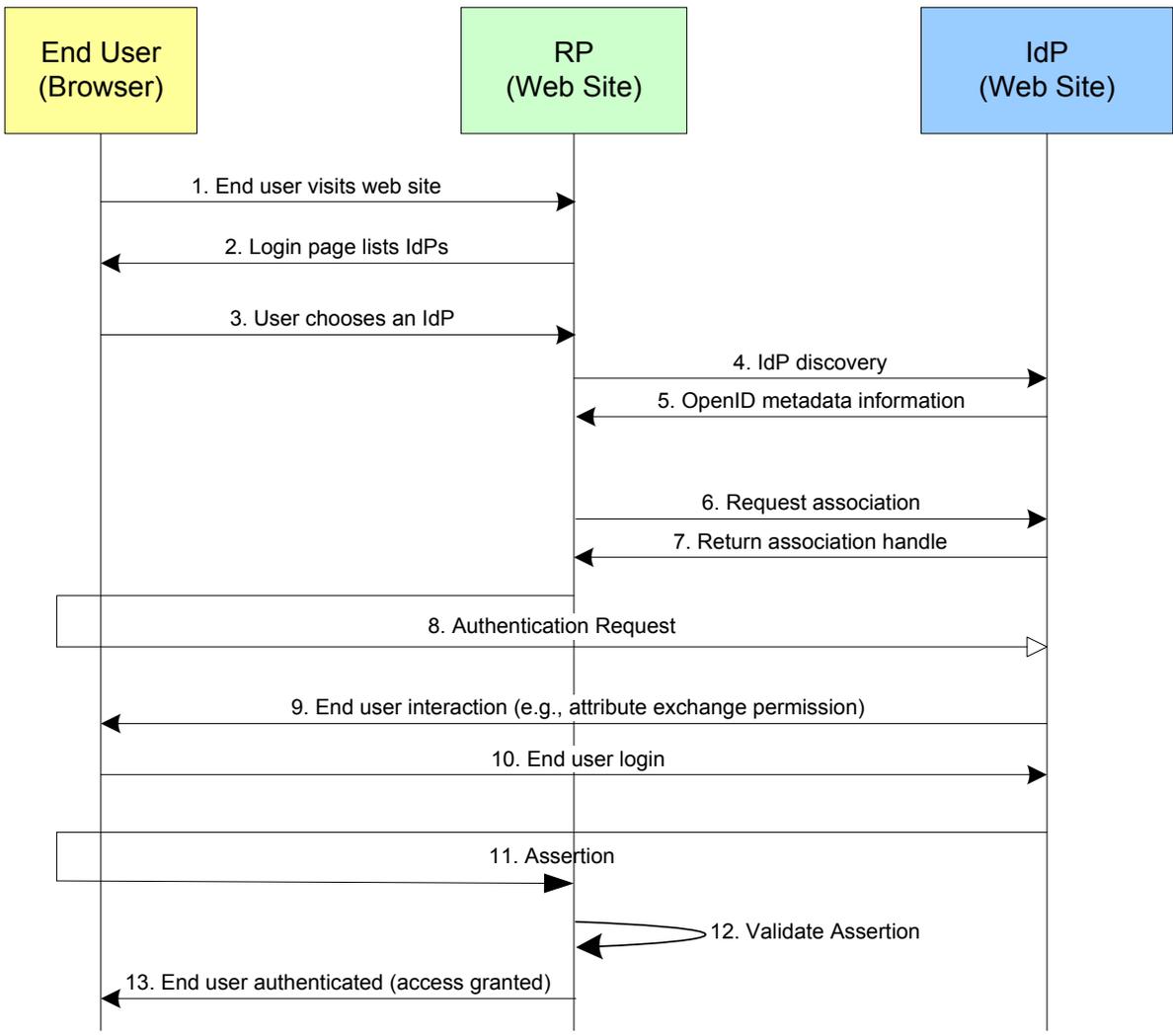
- Open Source roots
- OpenID Foundation serves as steward and provides necessary infrastructure
- Used/supported by JanRain, SixApart, Google, Yahoo, Facebook, AOL, MySpace, Novell, Sun, etc.
- 1 billion+ OpenID-enabled accounts
- 40,000+ web sites support OpenID

### ➤ Federal Profile

- Profile based on OpenID 2.0
- Requires SSL/TLS on all endpoints
- Requires *Directed Identity* Approach
- Requires pair-wise unique pseudonymous identifiers
- Requires short-lived association handles



## Portable Identity Schemes: OpenID





## Portable Identity Schemes: Information Card (IMI)

### ➤ Information Card

- Analogous to the cards you carry in wallet
- Open Source & industry standards
- Supported by Azigo, CA, Equifax, Google, Intel, Microsoft, Novell, Oracle, Paypal, etc.
- Built into MS Vista; option for XP
- Earlier stage of adoption than OpenID
- ALs 1 thru 3; possibly AL 4

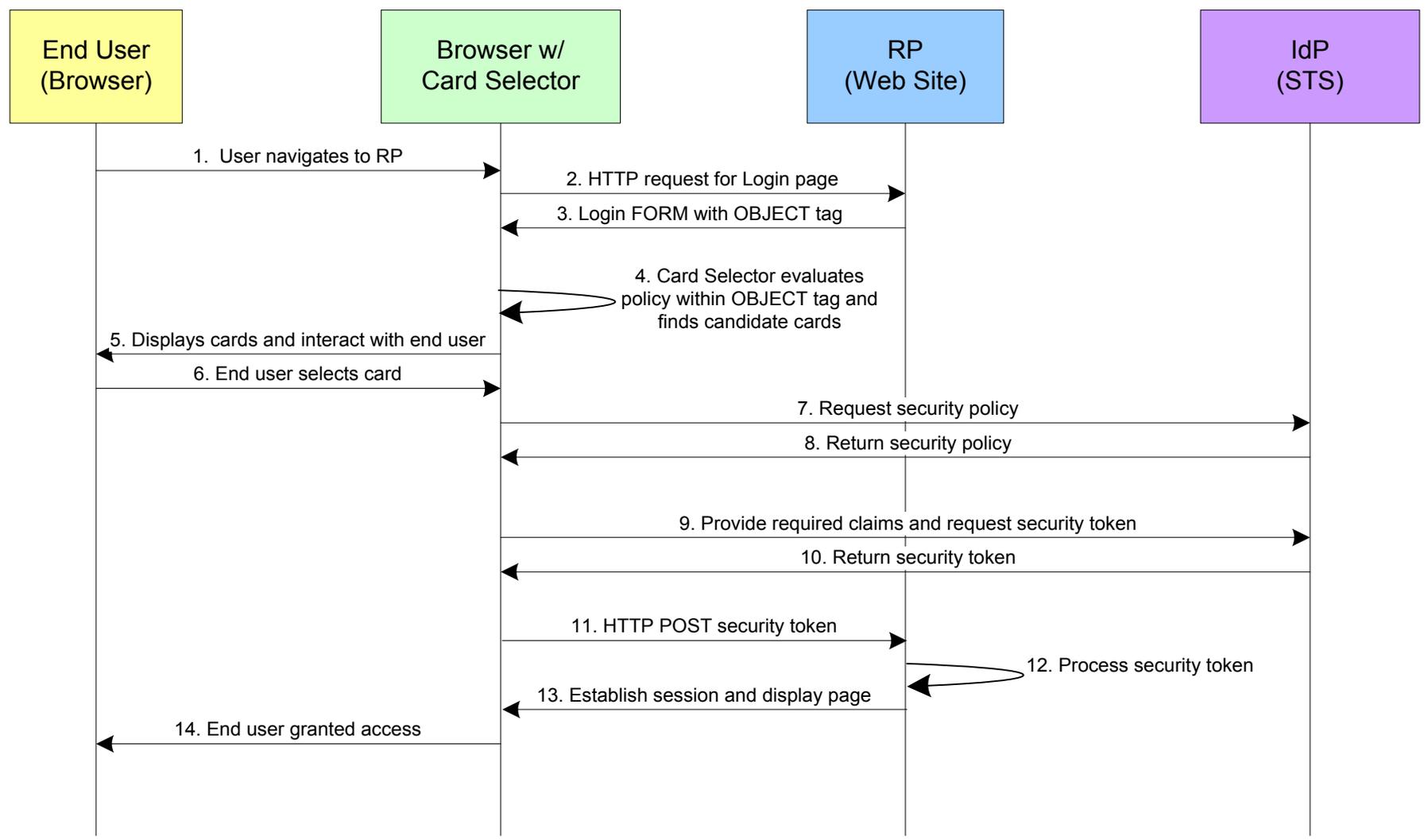
### ➤ Federal Profile

- Profile of *Identity Metasystem Interoperability Document 1.0* (IMI)
- Requires encryption of PII
- Requires use of optional *Private Personal Identifier* (PPID)
- Managed cards only



# Identity, Credential, and Access Management

## Portable Identity Schemes: Information Cards (IMI)





## Backup Slides

- Full Privacy Principles



## Trust Framework Privacy Principles

- 1. Opt In** Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of individual attributes for each transaction.
- 2. Minimalism** – Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile. RP Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002.



## Trust Framework Privacy Principles

- 3. Activity Tracking** – Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication. RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002.
- 4. Adequate Notice** – Identity Provider must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process.



## Trust Framework Privacy Principles

- 5. Non Compulsory** – As an alternative to 3rd-party identity providers, agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service.
- 6. Termination** – In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.



## Backup Slides

➤ [IDManagement.gov](https://www.idmanagement.gov)





# Identity, Credential, and Access Management

Browser window: IDManagement.gov - Mozilla Firefox  
 URL: http://idmanagement.gov/drilldown.cfm?action=openID\_openGOV  
 Today's Date: Tuesday - March 8, 2011



**Home Accessibility Contact Us RSS Feed**

**ABOUT US CALENDAR SITE MAP**

**Quick Click:**

Select a Link...

**Local IDManagement.gov Links:**

- Accessibility Policy
- Calendar
- Contact Us
- Home
- Library
- Links Policy
- Login to the ICAMSC page
- News
- Open ID Solutions for Open Govt
- Plug-In Policy
- Privacy Policy
- RSS Feed
- Sitemap

**Related Federal Government Sites:**

- ECA PKI Program
- Federal PKI Management Authority
- Federal PKI Policy Authority
- FIPS 201 Evaluation Program

**Open Identity Solutions for Open Government**

The Open Identity Initiative seeks to leverage existing industry credentials for Federal use. The Initiative approves credentials for government use through our Trust Framework Providers who assess industry Identity Providers (IDPs).

The [Trust Framework Provider Adoption Process](#) outlines the process that the ICAM community uses to sanctify organizations that assess commercial identity providers.

Trust Framework Providers:

- [Open Identity Exchange](#) - Level of Assurance 1 (Provisional Approval)
- [Kantara Initiative](#) - Level of Assurance 1, 2, and non-crypto 3 (Provisional Approval)
- InCommon Federation - Draft submission under review

The [Scheme Adoption Process](#) outlines the process that the ICAM community uses to develop and/or approve specification profiles for achieving portable identity over the Internet.

Adopted Schemes:

- [ICAM OpenID 2.0 Profile](#) - Fully adopted
- [ICAM IMI 1.0 Profile](#) - Fully adopted
- [ICAM SAML 2.0 Web Browser SSO Profile](#) - Fully adopted

Certified Identity Providers:

- Google - ICAM OpenID 2.0 Profile, Level of Assurance 1 - <http://google.com>
- Equifax - ICAM IMI 1.0 Profile, Level of Assurance 1 - <http://equifax.com>
- PayPal - ICAM OpenID 2.0 Profile, Level of Assurance 1 - <http://paypal.com>
- PayPal - ICAM IMI 1.0 Profile, Level of Assurance 1 - <http://paypal.com>
- VeriSign - ICAM OpenID 2.0 Profile, Level of Assurance 1 - <http://pip.verisignlabs.com>
- Wave Systems - ICAM OpenID 2.0 Profile, Level of Assurance 1 - <http://wave.com>

**What's Hot:**

**M-11-11: Continued Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors**

**Smartcard Issuance Progress by Agency:**

[Click here to view the statistics for 12/1/2010](#)

**Current Status - HSPD-12:**

[Click here to view the statistics as of 12/1/2010](#)

**Federal PKI Community Transition to SHA-256 FAQ:** [Click here for Ver 1.0](#)